524,772

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
26 février 2004 (26.02.2004)

PCT

(10) Numéro de publication internationale
WO 2004/017269 A1

(51) Classification internationale des brevets[7] : G07F 19/00

(21) Numéro de la demande internationale :
PCT/FR2003/002536

(22) Date de dépôt international : 14 août 2003 (14.08.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02/10367 16 août 2002 (16.08.2002) FR

(71) Déposants et
(72) Inventeurs : **DEBLOCK, Alain** [FR/FR]; 37, rue Carnot, F-78000 Versailles (FR). **BEHAGHEL, Thibault** [FR/FR]; 13, rue Saint Denis, F-92100 Boulogne (FR). **DE CHABANNES, Francois** [FR/FR]; 16, rue de l'Orangerie, F-78000 Versailles (FR). **JEANTEUR, Denis** [FR/FR]; 111, avenue de Verdun, F-92130 Issy-les-Moulineaux (FR).

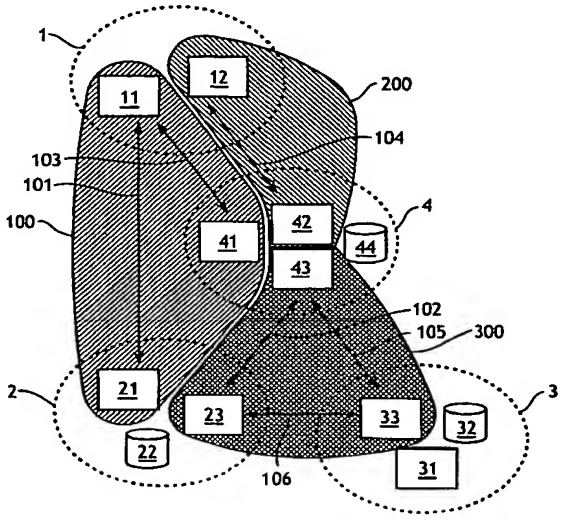
(74) Mandataire : **MARTIN, Jean-Jacques**; Cabinet Regimbeau, 20, rue de Chazelles, F-75847 Paris Cedex 17 (FR).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

[Suite sur la page suivante]

(54) Title: METHOD AND SYSTEM FOR THE SECURE TRANSMISSION OF A CONFIDENTIAL CODE THROUGH A TELECOMMUNICATION NETWORK

(54) Titre : PROCEDE ET SYSTEME DE SECURISATION DE TRANSMISSION D'INFORMATIONS SUR DES RESEAUX DE TELECOMMUNICATION



(57) Abstract: The invention relates to a method for the secured and automated transmission of confidential information, in particular an identification code to an authentication body (3) during a transaction with a user (1). The inventive method consists in transmitting a first part of confidential information to said authentication body through a first network and is characterised in that in the first stage, the user (1) transmits a second part of confidential information complementary to the first part thereof to a neutral intermediate party (4) through a second network (200) disjointed from the first network, afterwards, the neutral intermediate party (4) transmits the received complementary part of confidential information to the authentication body (3) through a third network (300).

[Suite sur la page suivante]

WO 2004/017269 A1

(84) **États désignés** *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *avec rapport de recherche internationale*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé : L'invention concerne un procédé de transmission sécurisée et automatisée d'une information confidentielle, notamment d'un code d'identification, à un organisme d'authentification (3) lors d'une transaction avec un utilisateur (1) selon lequel on transmet une première partie d'une information confidentielle à l'organisme d'authentification sur un premier réseau, caractérisé en ce qu'il comporte une étape selon laquelle l'utilisateur (1) transmet la deuxième partie de l'information confidentielle, complémentaire de la première partie, à un intermédiaire neutre (4) sur un deuxième réseau (200) disjoint du premier réseau, l'intermédiaire neutre (4) transmettant ensuite à l'organisme d'authentification (3), sur un troisième réseau (300), la partie complémentaire de l'information confidentielle qu'il a reçue.

PROCEDE ET SYSTEME DE SECURISATION DE TRANSMISSION D'INFORMATIONS SUR DES RESEAUX DE TELECOMMUNICATION.

DOMAINE TECHNIQUE GENERAL.

L'invention concerne un procédé automatisé de transmission sécurisée d'informations confidentielles, comportant éventuellement des codes d'identification, sur deux réseaux de télécommunication disjoints, et éventuellement non sécurisés, notamment Internet et le réseau téléphonique.

Plus précisément, l'invention concerne un procédé évitant le transit, le stockage et la reconstitution des informations confidentielles, dans leur intégralité, même de manière transitoire, par un ou plusieurs intermédiaires entre un expéditeur et un destinataire desdites informations confidentielles.

Le procédé permet en outre à un intermédiaire neutre de construire une trace de l'historique d'utilisation de l'information confidentielle, de manière anonyme et sans pour autant pouvoir la reconstituer dans son intégralité.

L'invention est particulièrement apte à la transmission d'un code de carte de paiement ou d'authentification dans le cadre de la sécurisation des paiements, et dans le cadre d'un accès distant à caractère confidentiel notamment, par transmission d'un mot de passe ou équivalent.

ETAT DE L'ART.

La transmission d'informations confidentielles, notamment de codes d'identification, sur des réseaux publics et particulièrement de numéros de cartes de paiement ou de mots de passe, est essentielle pour finaliser via ces réseaux les transactions à distance, notamment commerciales, ou pour s'identifier via ces réseaux.

Les utilisateurs, notamment les consommateurs en ligne, sont en effet réticents à transmettre les informations confidentielles, notamment leur numéro de carte de paiement ou leur mots de passe, sur Internet ou sur un autre réseau de télécommunication. Cette réticence est un frein important

au développement des transactions, notamment commerciales, sur ces réseaux.

Les craintes des utilisateurs sont notamment :

- d'une part, la crainte d'un piratage de leurs informations confidentielles, via une écoute du réseau lors de la transmission de ces informations confidentielles de l'expéditeur vers le destinataire. Le piratage peut être effectué par un tiers qui récupérerait ainsi l'information confidentielle ;

- d'autre part, la crainte du piratage de l'information confidentielle sur le serveur d'un intermédiaire, par exemple un prestataire de service, d'un marchand ou d'un tiers de confiance, ou simplement de la malhonnêteté du dit intermédiaire.

Ces deux craintes se résument par la peur que des personnes mal intentionnées puissent réutiliser cette information confidentielle, par exemple un numéro de carte de paiement ou un mot de passe, pour se faire passer pour l'utilisateur.

Ainsi, malgré la mise en place de systèmes de cryptage des données lors de leur transfert, la méfiance reste de mise.

Par ailleurs, dans le cas des achats en ligne par exemple, les craintes des fournisseurs de produits ou de services en ligne sont notamment :

- d'une part, la crainte de répudiations excessives des achats en ligne due à la fraude, et parfois à la malhonnêteté de certains utilisateurs, notamment des consommateurs en ligne;

- d'autre part, la crainte d'attaques sur leurs serveurs, par des tiers mal intentionnés qui veulent récupérer toutes sortes d'informations identifiantes comme par exemple des mots de passe ou des numéros de cartes de paiement. Les mesures de sécurité ne sont jamais suffisantes et des milliers de numéros de cartes de paiement, de mots de passe ou toutes autres informations confidentielles disponibles sur un serveur sont une cible très attractive pour des malfaiteurs.

Les solutions apportées à ce problème sont de trois types :

- soit un cryptage des données, au moins lors de la transmission, via des protocoles ou éventuellement matériels variés bien connus de l'homme de l'art comme par exemple, mais non limitativement, le protocole de transaction SSL ou « Secure Socket Layer» ou TLS « Transport Layer Security» selon la terminologie anglo-saxonne généralement utilisée par l'homme du métier, les protocoles SSL et TLS utilisant eux mêmes différents algorithmes de chiffrements, des protocoles d'authentification et des systèmes de génération de certificats.

- soit des procédés d'authentification avec inscription préalable chez un tiers de confiance ou équivalent et qui imposent généralement la divulgation d'informations personnelles. L'utilisateur doit faire alors confiance en la capacité de ces prestataires et intermédiaires d'assurer la sécurité de l'authentification. De tels exemples de procédés sont divulgués dans les documents US 6 012 144 ou FR 2 806 229 par exemple.

- soit des procédés dits « propriétaires » qui imposent l'adhésion de l'acheteur et du vendeur à un système technique, par exemple lecteur de carte ou système de génération de clef propriétaire, et qui nécessitent une installation d'un logiciel, plug-in ou d'un matériel. C'est le cas notamment du procédé divulgué dans le document WO 96/29667.

Les premières solutions de cryptage ne répondent pas aux craintes des utilisateurs puisque seule la transmission est sécurisée et que leurs informations confidentielles circulent toujours en un morceau (même si par exemple le protocole internet découpe l'information en paquets, ces derniers sont reconstitués et reconstituables) et sont stockées en un seul morceau. Par exemple le protocole de transmission sécurisée SSL permet une bonne protection de la transmission de données mais d'une part, il n'est pas impossible à décrypter, et d'autre part, il laisse intact le problème à l'émission et à la réception des données. De plus, les utilisateurs ne perçoivent pas forcément la sécurité du système car il a été montré, notamment sur Internet, que de tels systèmes, basés sur la transmission intégrale et par une seule ou plusieurs voies de mêmes technologies, étaient une source de fraude.

Les secondes solutions à pré inscription ne conviennent pas à l'utilisateur car elles ne sont pas universelles et lui demandent des efforts d'inscription. Les secondes solutions ne conviennent pas non plus aux fournisseurs de produits ou services qui recherchent des solutions sans rupture de flux, c'est à dire où la transaction est fluide, notamment pour l'utilisateur.

Enfin, les solutions du troisième type nécessitent un effet d'enrôlement de masse, notamment des consommateurs, et de plus elles requièrent bien souvent un investissement financier ou en temps de la part de l'utilisateur pour en maîtriser l'installation ou l'usage. Finalement, ces solutions se sont également avérées bien souvent très coûteuses pour le prestataire de service, le marchand ou l'organisme d'authentification.

Par ailleurs, on constate que la transmission des informations confidentielles par télécopie, téléphone, SMS, courrier et tout autre moyen de communication à distance, électronique ou autre, rassure certains utilisateurs bien que le risque de piratage des informations confidentielles dans ces cas soit très élevé et que ces solutions ne résolvent pas le problème du stockage des informations.

En conclusion la transmission d'une information confidentielle sur un réseau comporte un risque au cours des étapes suivantes :

- la saisie de cette information sur un même terminal car le terminal (clavier, écran, etc...) peut être espionné ;
- la transmission sur le réseau notamment le début et la fin car l'information même cryptée peut être capturée puis soit réutilisée directement soit décryptée ;
- le stockage de cette information confidentielle chez un intermédiaire, tiers de confiance ou fournisseur de produits ou services, car ce serveur peut être un point faible de sécurité malgré les précautions prises et même si un algorithme de cryptage, surtout s'il est de type réversible, est appliqué ;
- les phases d'inscription sont particulièrement vulnérables, car en plus de l'information confidentielle sont souvent transmises des informations personnelles.

PRESENTATION DE L'INVENTION.

L'invention propose de pallier les inconvénients évoqués précédemment.

Un but de l'invention est d'assurer la transmission d'une information confidentielle ne nuisant pas à la fluidité de la transaction et étant très convivial pour l'utilisateur.

Un autre but de l'invention est de proposer une technique permettant de guider l'utilisateur dans les différentes étapes de la transmission d'informations.

Un autre but de l'invention est de fournir un procédé qui ne nécessite pas d'inscription préalable auprès de l'intermédiaire neutre assurant le transfert anonyme d'au moins une partie de l'information confidentielle. Elle s'oppose donc partiellement à la notion bien connue de l'homme du métier de 'tiers de confiance' au sens ou le tiers de confiance est bien souvent dépositaire d'informations personnelles pouvant également être confidentielles.

Un autre but de l'invention est de fournir un procédé ne nécéssitant pas en lui-même d'installations particulières chez l'utilisateur autre que les logiciels, matériels et moyens permettant de communiquer sur des réseaux mis en œuvre lors de la transaction. Ainsi, la sécurisation de la transaction ne s'effectue pas au détriment de la fluidité de la transaction.

Un autre but de l'invention est de permettre une meilleure identification de l'utilisateur lors de la transmission d'informations confidentielles tout en conservant une simplicité d'usage et en assurant l'anonymat de l'utilisateur.

Selon cette invention la sécurité est assurée par la séparation de l'information en deux parties complémentaires non signifiantes séparément, véhiculée sur deux réseaux disjoints via un intermédiaire neutre et ne nécessitant ni inscription de l'utilisateur chez cet intermédiaire neutre, ni installation par l'utilisateur de logiciels et de matériels autres que ceux nécessaires à la connexion sur les deux réseaux de télécommunication.

A cet effet, l'invention propose un procédé de transmission sécurisée d'informations confidentielles, notamment d'un code d'identification, à un organisme d'authentification ou tout autre destinataire final, dit « organisme d'authentification », habilité à recevoir cette information lors d'une transaction avec un utilisateur. Ce procédé est caractérisé en ce que l'utilisateur sépare l'information confidentielle qu'il veut transmettre à l'organisme d'authentification en deux parties complémentaires qui n'ont pas de valeur prises séparément.

On utilise ainsi une technique de sécurité disjointe permettant de transmettre de manière simultanée et entièrement automatisée deux parties complémentaires d'une information confidentielle sur deux réseaux différents. Cette technique est un moyen très sûr de transmission d'informations confidentielles si les parties véhiculées sont sans valeur prises séparément et s'il est impossible à un tiers de recoller les morceaux ce que permet le procédé mis en œuvre par l'invention.

Le procédé mis en œuvre par l'invention met en place un intermédiaire, appelé « intermédiaire neutre », qui permet de transmettre de manière anonyme et sans stockage d'informations susceptibles d'être reconstituées, une partie non utilisable seule d'une information confidentielle, notamment un code d'identification, via un réseau dit « le deuxième réseau » distinct technologiquement du réseau dit « le premier réseau » qui sert quant à lui à transmettre l'autre partie complémentaire de cette information confidentielle directement ou indirectement vers l'organisme authentificateur.

Dans ce procédé les données stockées par l'intermédiaire neutre le sont selon des techniques de cryptage non réversible dit « empreintes numériques » bien connues de l'homme du métier, comme par exemple l'algorithme MD5 (« Message Digest 5» selon la terminologie anglo-saxonne et référencé RFC1321) ou SHA1 (« US Secure Hash Algorithm 1» selon la terminologie anglo-saxonne et référencé RFC3174) ou tout autre algorithme de cryptage à sens unique. Ainsi l'intermédiaire neutre ne peut pas reconstituer les informations qu'il stocke. Cette 'identification anonyme'

se fait par comparaison d'empreintes numériques stockées avec l'empreinte numérique d'une combinaison identique des données transmises. A ce titre, le procédé permet de bâtir un historique anonyme des transactions en stockant, par exemple, l'empreinte numérique d'une combinaison des coordonnées de l'utilisateur sur le deuxième réseau avec la partie complémentaire de l'information confidentielle reçue par l'intermédiaire neutre également sur le deuxième réseau. A cette empreinte numérique peuvent être associées des données statistiques de toutes sortes à des fins de classement, d'analyse et de détermination de scores.

L'utilisateur transmet une première partie de l'information confidentielle soit directement à l'organisme d'authentification, soit via un intermédiaire, par exemple un fournisseur de produits ou de services sur un premier réseau, par exemple Internet.

A la demande de l'intermédiaire neutre, lui-même sollicité directement ou indirectement par l'organisme d'authentification, l'utilisateur transmet alors la deuxième partie complémentaire du code confidentiel à l'intermédiaire neutre sur un deuxième réseau disjoint du premier et utilisant par exemple des technologies ou protocoles de communication différents, l'intermédiaire neutre transmettant ensuite à l'organisme d'authentification la partie du code qu'il a reçu.

Les échanges avec l'organisme d'authentification et éventuellement avec les fournisseurs de produits ou de services intervenant dans la transaction avec l'utilisateur sont sécurisés point à point par des techniques de codage et de reconnaissance mutuelles bien connues de l'homme du métier, comme par exemple l'échange de certificats ou de clés, la transmission SSL, TLS, etc. Ce réseau sécurisé entre deux points est dit « troisième réseau». Les premier et deuxième réseaux sont des réseaux liés à l'utilisateur alors que le troisième est un réseau entre l'intermédiaire neutre, l'organisme d'authentification et éventuellement des fournisseurs de produits ou services intervenants dans la transaction.

Cette séparation de l'information en deux parties complémentaires, transmises par des voies de communication disjointes et de technologies

différentes comme par exemple l'Internet et le téléphone, est facilement compréhensible par l'utilisateur qui transmet une partie de son information confidentielle par des moyens de télécommunication distincts. Il en est naturellement rassuré.

Les deux réseaux possèdent des moyens d'entrée de données disjoints qui peuvent être par exemple et non limitativement un clavier d'ordinateur, les touches d'un téléphone, un système de reconnaissance vocale, un lecteur de carte, etc. Ceci permet d'éviter le piratage ou l'écoute des données entrées par un terminal unique et notamment un clavier d'ordinateur.

L'invention est avantageusement complétée par les caractéristiques suivantes, prises seules ou en une quelconque de leurs combinaisons techniquement possible :

- la transmission de la première partie de l'information confidentielle à l'organisme d'authentification s'effectue selon les étapes suivantes :
  - l'utilisateur transmet la première partie de l'information confidentielle à un fournisseur de produits ou de services sur le premier réseau ;
  - le fournisseur transmet ensuite la première partie à l'organisme sur un troisième réseau ;
- au moins un identifiant de session, partagés entre au moins deux des acteurs de la transaction, permettent à l'organisme d'authentification de reconstituer automatiquement l'information confidentielle que l'utilisateur lui transmet ;
- chaque identifiant de session est généré par au moins un des acteurs de la transaction ;
- l'intermédiaire neutre contacte automatiquement l'utilisateur sur le deuxième réseau pour récupérer la deuxième partie complémentaire de l'information confidentielle ;
- la communication sur le premier réseau entre l'utilisateur et l'organisme d'authentification ou le fournisseur de produits ou de service est transférée automatiquement vers l'intermédiaire neutre de transaction ;

- l'utilisateur contacte l'intermédiaire neutre sur le réseau pour transmettre la deuxième partie complémentaire de l'information confidentielle associée avec un identifiant de session ;
- des coordonnées de rappel de l'utilisateur sur le deuxième réseau sont transmises à l'intermédiaire neutre par l'organisme d'authentification sur le troisième réseau ;
- des coordonnées de rappel de l'utilisateur sur le deuxième réseau sont transmises à l'intermédiaire neutre par le fournisseur de produits ou services sur le troisième réseau ;
- des coordonnées de rappel de l'utilisateur sur le deuxième réseau sont transmises à l'intermédiaire neutre par l'utilisateur sur le premier réseau ;
- le troisième réseau est un réseau sécurisé point à point ;
- l'utilisateur est guidé automatiquement par l'intermédiaire neutre dans les différentes étapes du procédé de transmission de la deuxième partie de l'information confidentielle sur les premier et/ou deuxième réseaux respectivement, de manière coordonnée et éventuellement synchronisée.
- l'intermédiaire neutre établit un historique des transactions ;
- l'historique établi par l'intermédiaire neutre est anonyme ;
- l'anonymat de l'historique est assuré par un codage non décryptable d'une combinaison des coordonnées de l'utilisateur sur le deuxième réseau et de la deuxième partie de l'information confidentielle transmise par l'utilisateur à l'intermédiaire neutre sur le deuxième réseau ;
- l'intermédiaire neutre émet un avis lié à l'historique de transaction de l'utilisateur sur le réseau ;
- l'intermédiaire neutre demande à l'utilisateur de fournir, en outre de l'information confidentielle à transmettre à l'organisme, un code personnel qui est utilisé lors des transactions ultérieures et qui permet d'identifier l'utilisateur ;
- le code personnel est transmis, par un réseau du type sécurisé point à point, à un deuxième organisme d'authentification auprès duquel l'utilisateur est préalablement inscrit ou connu ;
- le code personnel est un code numérique et/ou vocal rentré sur un terminal en connexion avec le deuxième réseau ;

- l'intermédiaire neutre stocke en clair ou en crypté de manière réversible les coordonnées de l'utilisateur sur le réseau ;
- l'intermédiaire neutre stocke en clair ou de manière réversible la deuxième partie complémentaire de l'information confidentielle fournie par l'utilisateur sur le réseau ;
- l'intermédiaire neutre recontacte l'utilisateur après que ce dernier s'est déconnecté du premier réseau, ladite connexion au premier réseau étant rétablie une fois que la deuxième partie de l'information confidentielle a été transmise à l'intermédiaire neutre.

Les principaux avantages de l'invention sont, de manière non limitative, les suivants :

- la sécurisation de la transmission d'informations par deux voies distinctes utilisant deux réseaux disjoints mettant en œuvre par exemple deux technologies ou protocoles de communication différents,
- la mise en confiance de l'utilisateur pour transmettre des informations confidentielles, notamment son numéro de carte de paiement ou son mot de passe, en lui permettant de visualiser le processus assurant la sécurité,
- la facilité d'usage pour l'utilisateur par l'automatisation du processus et l'utilisation d'interfaces de guidage éventuellement coordonnées en temps réel sur les deux réseaux,
- la sécurisation de la saisie de l'information confidentielle par l'utilisation de deux terminaux d'entrée des données disjoints,
- l'identification de l'utilisateur par connexion des moyens formant serveur de l'intermédiaire neutre vers l'utilisateur,
- la possibilité de bâtir un historique anonyme des transactions en utilisant des empreintes numériques,
- la possibilité d'une deuxième identification éventuellement par un deuxième organisme d'authentification afin de renforcer le niveau d'identification,
- la sécurité et la confidentialité des transmissions entre l'intermédiaire neutre et l'organisme d'authentification ou éventuellement un prestataire de service ou un marchand par l'utilisation de transmission point à point.

L'invention concerne également un système pour la mise en œuvre du procédé selon l'invention.

PRESENTATION DES FIGURES

D'autres caractéristiques, buts et avantages de l'invention ressortiront de la description qui suit qui est purement illustrative et non limitative et qui doit être lue en regard des dessins annexés sur lesquels :

- la figure 1 représente schématiquement les échanges d'informations entre un utilisateur, un fournisseur de produits ou de service, par exemple un marchand, un organisme d'authentification, par exemple une banque, et l'intermédiaire neutre;
- la figure 2 représente schématiquement les différentes étapes d'un procédé de sécurisation des échanges d'informations entre un utilisateur, un fournisseur de produits ou services, par exemple un marchand, un organisme d'authentification, par exemple une banque, et l'intermédiaire de sécurisation ; et
- la figure 3 représente schématiquement un enchaînement possible des différentes étapes d'un procédé de sécurisation des échanges d'informations entre un utilisateur, un fournisseur de bien et de services, par exemple un marchand, un organisme d'authentification, par exemple une banque et l'intermédiaire neutre.

DESCRIPTION DETAILLEE.

La figure 1 représente schématiquement les échanges d'informations entre un utilisateur 1, un fournisseur de produits ou services 2, un organisme d'authentification 3 et l'intermédiaire neutre 4 lors d'une transaction quelconque en ligne sur un réseau de télécommunication. Il faut noter ici que le transit d'une partie de l'information confidentielle via le fournisseur de produits ou services n'est pas indispensable à la transmission de l'information. Cette transmission peut se faire directement vers l'organisme d'authentification. En effet la sécurité et l'anonymat de la transmission reposant sur les échanges entre l'utilisateur 1, l'intermédiaire neutre 4 et l'organisme d'authentification 3, la voie de transmission de l'autre partie de l'information confidentielle est moins importante.

La figure 1 présente des réseaux de communication comportant deux réseaux disjoints et utilisant par exemple des technologies ou protocoles de communication différents formant les parties 100 et 200, et un réseau privé ou sécurisé point à point formant la partie 300.

Les doubles flèches 102, 105 et 106 symbolisent les échanges d'informations entre le fournisseur de produits ou services 2 et l'intermédiaire neutre 4, l'intermédiaire neutre 4 et l'organisme d'authentification 3, et le fournisseur de produits ou services 2 et l'organisme d'authentification 3 respectivement. Le lien 102 est optionnel car toutes les informations nécessaires à l'activation de la transmission sur le deuxième réseau peuvent transiter par l'organisme authentificateur 3.

La première partie possible 100 du réseau de télécommunication permet une communication entre l'utilisateur 1 et le fournisseur de produits ou services 2 représentée par la double flèche 101, ainsi qu'entre l'utilisateur 1 et l'intermédiaire neutre 4 lors d'échanges 103. Elle est préférentiellement du type Internet et éventuellement, mais non nécessairement, sécurisée. La première partie 100 peut donc supporter tout type de caractères devant être transmis par l'utilisateur 1. La première partie 100 est nécessairement disjointe de la partie 200 et utilise par exemple des technologies ou protocoles de communication différents de la partie 200.

Dans les développements qui vont suivre, on désigne par Internet tous les réseaux informatiques 100 de terminal informatique à terminal informatique. La désignation comprend notamment toutes sortes de réseaux privés ou publics, comme intranet ou extranet par exemple.

La deuxième partie possible 200 du réseau de télécommunication permet une communication entre l'utilisateur 1 et l'intermédiaire neutre 4 lors d'échange 104. Elle est préférentiellement du type réseau téléphonique. La deuxième partie 200 est nécessairement disjointe de la partie 100 et utilise par exemple des technologies ou protocoles de communication différents de la partie 100.

Le réseau téléphonique est, dans l'état de l'art actuel, composé essentiellement de terminaux de téléphonie à touches numériques. Ainsi,

les données transmises par les terminaux sont numériques dans l'état de l'art actuel. L'évolution de l'état de l'art pouvant permettre prochainement la transmission de tout type de caractères.

Ainsi, à l'extrémité du réseau 100 située près de l'utilisateur 1, le système de mise en œuvre du procédé possible selon l'invention comporte d'une part des moyens 11 de connexion au réseau 100 et d'autre part des moyens de connexion 12 au réseau 200.

Les moyens 11 communiquent avec des moyens 21 situés chez le fournisseur de produits ou services 2 et des moyens 41 situés chez le l'intermédiaire neutre 4, afin de permettre les échanges 101 et 103 respectivement.

Les moyens 12 communiquent avec des moyens 42 situés chez l'intermédiaire neutre 4, afin de permettre les échanges 104 sur la partie 200 du réseau.

Les moyens 11 comportent par exemple un terminal informatique dit « terminal web », puisque le réseau 100 est préférentiellement du type Internet.

Les moyens 12 comportent par exemple des moyens formant une connexion téléphonique fixe ou un téléphone mobile puisque le réseau 200 est préférentiellement du type réseau de téléphonie fixe ou mobile.

Le téléphone 12 est avantageusement à touches et permet l'envoi de codes DTMF « Dual Tone Multi-Frequency» selon la terminologie anglo-saxonne généralement utilisée ou tout autre protocole ou méthode disponible sur ce moyen pour transmettre la partie de l'information confidentielle.

Le procédé selon l'invention est ainsi transposable aux systèmes déjà existants, puisque les téléphones mobiles permettent l'envoi de codes DTMF et la très grande majorité des téléphones fixes sont maintenant à touches et fréquence vocale permettant l'envoi de codes DTMF.

Dans le cas où les moyens 12 de l'utilisateur 1 ne permettraient pas la transmission des codes DTMF, une variante du procédé selon l'invention, utilise la reconnaissance vocale pour acquérir la deuxième partie de l'information confidentielle.

A l'extrémité du réseau 100 située près du fournisseur de produits ou services 2, le système comporte des moyens 21 formant serveur sur le réseau 100. Les moyens 21 comportent par exemple un serveur dit « serveur web ».

Le fournisseur de produits ou services 2 peut ainsi échanger des données 101 avec l'utilisateur 1.

La troisième partie 300 du réseau de télécommunication est préférentiellement du type apte à la transmission de données sécurisées point à point.

A titre d'exemple non limitatif, ce peut être un réseau de type VPN (Virtual Private Network), un réseau privé, un protocole de transmission sécurisé point à point qui peuvent utiliser, par exemple, des messages signés par un MAC (Message Authentification Code) qui est un scellement calculé avec un algorithme, par exemple de type DES (Data Encryption Standard), et associé à une clé de scellement échangée avec les données. Cela peut être également des transmissions SSL ou TLS avec échange de certificats entre les deux protagonistes.

D'autres procédés de transactions sécurisées point à point sont bien entendu connus de l'homme du métier et peuvent être applicables au procédé. Eventuellement de nouveaux procédés de sécurité peuvent se substituer aux protocoles connus actuellement.

Ainsi, le système chez le fournisseur de produits ou services 2 peut comporter des moyens 23 aptes à gérer des transactions point à point 102, 106.

Encore une fois, le procédé selon l'invention est transposable aux systèmes de l'art antérieur, puisque la plupart des fournisseurs de produits ou services notamment sur Internet sont équipés de tels serveurs. Ils utilisent souvent déjà des protocoles de transfert sécurisé de données point à point.

Dans le cas où le fournisseur de produits ou service 2 ne posséderait pas les moyens 23 aptes à la gestion de telles transactions, il en confie la prestation à un tiers agréé par l'organisme d'authentification 3. Ledit tiers a

mis au préalable en place avec l'organisme authentificateur 3 les protocoles adéquats de transfert.

Les moyens 21 et 23 de l'organisme d'authentification 2 sont gérés par des moyens 22.

Les systèmes aux extrémités du réseau 300 situées chez l'organisme d'authentification 3 et l'intermédiaire neutre 4 comportent des moyens 33 et 43 respectivement permettant le traitement des flux d'information en transfert sécurisé point à point.

De plus l'organisme d'authentification 3 possède des moyens 31 formant serveur d'authentification, ainsi que des moyens 32 permettant la gestion de l'ensemble des moyens 31 et 33.

On rappelle ici que le terme « organisme d'authentification» fait référence à un organisme bancaire ou financier, mais plus généralement à un organisme habilité à effectuer une authentification quelconque.

L'intermédiaire neutre 4 est relié aux moyens 12 sur le réseau 200 par l'intermédiaire de moyens 42 formant serveur. Les moyens 42 comportent par exemple un serveur téléphonique comme par exemple des moyens IVR (Interactive Voice Response) ou équivalents bien connus de l'homme du métier.

Les moyens 42 sont aptes par exemple à effectuer des appels téléphoniques 104, faire des appels différés, filtrer les codes DTMF, diffuser des messages et enregistrer des appels ainsi que toutes possibilités offertes par les systèmes informatiques couplés à la téléphonie pour échanger des informations avec l'utilisateur 1. Les moyens 42 sont connus de l'homme du métier.

De plus, l'intermédiaire neutre 4 est relié aux moyens 11 sur le réseau 100 par l'intermédiaire de moyens 41 formant serveur. Les moyens 41 comportent par exemple un serveur web.

Enfin, l'intermédiaire neutre 4 est relié aux moyens 33 sur le réseau 300 par l'intermédiaire de moyens 43 formant serveur point à point.

La transmission d'une partie complémentaire des données confidentielles via le fournisseur de produits ou services 2 est possible et souvent mise en œuvre, mais non indispensable au fonctionnement du

procédé présenté qui ne repose pas sur la sécurité de cette voie de transmission, et peut donc avantageusement s'effectuer directement vers l'organisme d'authentification 3.

Dans la présente description, le terme «d'information confidentielle» désigne tous les types de codes alphanumériques, numériques ou binaires confidentiels et/ou informations liées à une indentification ou transmission secrète. Cela peut être par exemple, mais non limitativement, un numéro de carte de paiement ou un code d'authentification propre à un système de sécurité.

Préférentiellement, la partie de l'information confidentielle transmise par le réseau téléphonique est numérique dans l'état de l'art actuel. L'autre partie de l'information confidentielle est, quant à elle, préférentiellement alphanumérique si les réseaux le supportent.

Les termes « début de l'information confidentielle » et « fin de l'information confidentielle » ou plus généralement « partie de l'information confidentielle » désignent deux parties disjointes de l'information confidentielle. Les parties disjointes n'ont pas de signification lorsqu'elles sont prises séparément et ne peuvent être reconstituées dans un procédé selon l'invention, puisqu'elles transitent par des chemins différents, et ne sont reconstituées que par l'organisme authentificateur 3.

La taille des différentes parties est indifférente, tant que ces deux parties sont strictement complémentaires et non significatives en terme d'identification ou de confidentialité lorsqu'elles sont prises séparément. Elles ne sont donc pas forcément de la même taille.

Préférentiellement, on utilise, dans un mode de mise en œuvre possible du procédé, deux acteurs, à savoir le fournisseur de produits ou services 2 et l'intermédiaire neutre 4, pour la transmission des informations confidentielles entre l'utilisateur 1 et l'organisme d'authentification 3.

Le fournisseur de produits ou services 2 et l'intermédiaire neutre 4 sont en communication avec l'utilisateur 1 selon deux modes de communication utilisant par exemple des technologies ou protocoles de communication différents, respectivement le réseau Internet 100 et le réseau téléphonique 200.

Ainsi, chacun transmet à l'organisme d'authentification 3, et par le réseau 300, une des deux parties de l'information confidentielle.

Les flux d'informations échangées entre les différents acteurs sont représentés schématiquement par les doubles flèches 101, 102, 103, 104, 105 et 106.

Les flux sont décrits de façon plus détaillée sur la figure 3, laquelle reprend les mêmes numérotations qu'aux figures 1 et 2 pour des éléments identiques.

Les figures 1 et 3 représentent des modes de mise en œuvre possibles de l'invention dans lesquels les différents acteurs sont des entités différentes.

Cependant, il est possible que la voie de transmission utilisateur 1 vers l'organisme d'authentification 3 via le fournisseur de produits ou services 2 soit simplifiée si la transmission de l'information confidentielle s'effectue directement entre l'utilisateur 1 et l'organisme d'authentification 3. Dans ce cas, les moyens des acteurs 2 et 3 sont regroupés dans l'organisme d'authentification 3. Dans ce cas, les différents serveurs présentés comme utiles pour la réalisation du procédé peuvent fonctionner sur le même moyen ou même faire partie intégrante d'un même programme. Les modes de transfert entre les différents acteurs restent les mêmes que ceux visibles aux figures 1 et 3.

En effet selon ce procédé c'est la voie via l'intermédiaire neutre 4 qui est primordiale pour assurer la sécurisation de la transmission de l'information confidentielle.

Dans tous les modes de mise en œuvre du procédé selon l'invention, aucune inscription préalable de l'utilisateur 1 n'est nécessaire.

L'invention est utilisable pour des transactions de commerce électronique, et de manière plus générale, pour tout processus d'authentification et de transfert de données.

Avantageusement, le procédé comporte les étapes selon lesquelles :

- L'utilisateur 1 sépare l'information confidentielle en deux parties complémentaires et distinctes, mais inutilisables indépendamment l'une de l'autre ;

- L'utilisateur 1 transmet chacune des deux parties du code par des moyens de communication distincts, par le réseau 100 au fournisseur de produits ou services 2, et par le réseau 200 à l'intermédiaire neutre 4. Dans la présente description, la transmission d'une partie de l'information confidentielle au fournisseur de produits ou services 2 est effectuée par exemple par un réseau Internet et la transmission de l'autre partie de l'information confidentielle à l'intermédiaire neutre 4 est effectuée par exemple par un réseau téléphonique. Avantageusement, les informations transmises sur les réseaux sont non réconciliables par un tiers. On rend ainsi sans valeur le piratage et l'écoute des communications ;
- Le fournisseur de produits ou de services 2 et l'intermédiaire neutre 4 transmettent à l'organisme d'authentification 3 la partie de code qui leur a été transmise par l'utilisateur 1.

Ainsi, selon le procédé de l'invention, seul l'organisme d'authentification 3 récupère l'intégralité de l'information. Ni le fournisseur de produits ou services 2, ni l'intermédiaire neutre 4 n'ont accès à l'intégralité de l'information.

Les deux parties de l'information, une fois réunies par l'organisme d'authentification 3, ne transitent plus que sur des réseaux privés ou sécurisés réputés non accessibles.

De fait, aucun intermédiaire n'a connaissance de l'ensemble de l'information confidentielle, et aucun ne peut stocker l'intégralité du code confidentiel.

L'invention concerne également l'utilisation qui peut être faite par l'intermédiaire neutre 4 d'empreintes numériques de couples formés par les coordonnées de l'utilisateur 1 sur le réseau 200, par exemple le numéro de téléphone, et une partie non signifiante d'informations confidentielles reçue par l'intermédiaire neutre de l'utilisateur 1.

Lors de chaque transaction, l'intermédiaire neutre 4 peut stocker ces empreintes numériques dans une base de données ou équivalent, par exemple comprise dans les moyens 44.

Ces empreintes numériques permettent de construire au niveau de l'intermédiaire neutre 4 un historique des transactions pouvant être utilisé,

non seulement à des fins de statistique ou reporting, mais aussi par exemple à des fins de qualification du risque potentiel client, en fonction du bon règlement ou non de la transaction lors des tentatives antérieures.

Les données sont stockées sous une forme d'empreinte numérique, par exemple en utilisant un mécanisme de type MD5 ou SHA1.

L'historique ainsi créé ou les données statistiques associées à cet historique pourront éventuellement être fournis au fournisseur de produits ou services 2 ou à l'organisme d'authentification 3 lorsqu'un utilisateur transmet à l'intermédiaire neutre 4 un couple constitué d'une même partie d'information et en utilisant les mêmes coordonnées sur le réseau 200 et dont l'empreinte numérique est stockée par l'intermédiaire neutre 4. Ainsi, l'intermédiaire 4 peut indiquer au fournisseur de produits ou services 2 si sont associés à ce couple des problèmes de paiement par exemple.

De même, il est possible d'indiquer au fournisseur de produits ou services 2 ou à l'organisme d'authentification 3 si c'est la première fois qu'un tel couple est entré.

On indique ainsi au fournisseur de produits ou services 2 ou à l'organisme authentificateur 3 les transactions qui présentent un risque.

En tout état de cause, le fait de devoir fournir dans le mode de réalisation préféré un numéro de téléphone, qui a une traçabilité relativement importante, permet de décourager une certaine catégorie de clients malhonnêtes.

L'intermédiaire neutre 4 ne stocke pas en clair les coordonnées de l'utilisateur 1 sur le réseau 200 sauf des coordonnées appartenant à une liste de numéros interdits, comme par exemple les numéros de cabines téléphoniques publiques ou des numéros utilisés par des fraudeurs potentiels ou jugés à risque. Potentiellement aucune transmission d'information ne sera possible à partir de ces coordonnées.

Il est ainsi possible de sécuriser les transactions, et de réduire les prix des polices d'assurance qu'est souvent amené à contracter le fournisseur de produits ou services 2 dans la situation de l'art antérieur.

On va maintenant décrire plus en détail les différentes étapes du procédé selon l'invention. L'exemple suivant présente une possibilité

d'intégration mais ne couvre pas l'ensemble du champ des applications possible du procédé. Par exemple, il s'agit dans cet exemple de règlement d'achats en ligne par carte de paiement, mais il pourrait également s'agir d'une authentification quelconque, sans qu'il y ait forcément achat. Ainsi le code à transmettre n'est pas forcément le numéro d'une carte de paiement.

La figure 2 présente un mode de mise en œuvre d'une transaction sur un premier réseau du type Internet et un deuxième de type téléphonique.

La figure 3 reprend schématiquement, et avec les mêmes références numériques, les flux d'informations s'échangeant entre les différents acteurs lors de la mise en œuvre du procédé selon les étapes de la figure 2.

A l'étape 201 de la figure 2, après avoir par exemple sélectionné des articles dans le catalogue d'un fournisseur de produits ou services 2, l'utilisateur 1 décide de valider son panier d'articles.

A l'étape 202, au cours du processus de validation de la commande, le fournisseur de produits ou services 2 demande à l'utilisateur 1 de lui transmettre les informations nécessaires à l'envoi et au paiement des produits de la commande.

Parmi ces informations, le fournisseur de produits ou services 2 ne demande que par exemple les huit premiers chiffres du numéro de carte de paiement de l'utilisateur 1. La transaction s'effectue de préférence en mode sécurisé type SSL.

A l'étape 203, l'utilisateur 1 envoie les informations demandées au fournisseur de produits ou services 2.

A l'étape 204, le fournisseur de produits ou services 2 génère un identifiant de session. C'est un identifiant propre à la transaction. Il va permettre aux différents acteurs d'échanger des informations relatives à cette transaction. Cet identifiant peut, selon une variante, être généré par l'organisme d'authentification 3 en réponse à la demande du fournisseur de produits ou services 2, lors des étapes 205 ou 207 détaillées plus bas.

A ce stade, le fournisseur de produits ou services 2 peut stocker les informations en attente de paiement dans une base de données, par exemple comprise dans les moyens 22, avec, par exemple, pour clé l'identifiant de session.

A l'étape 205, le fournisseur de produits ou services 2 envoie à l'organisme d'authentification 3 la première partie du numéro de carte de paiement accompagnée de l'identifiant de session si c'est lui qui l'a généré, ainsi que les autres données nécessaires pour finaliser la transaction avec l'organisme d'authentification 3. Les autres informations nécessaires sont par exemple la date d'expiration de validité de la carte paiement, le montant de la transaction, etc.

Les données nécessaires à l'organisme d'authentification 3 sont transmises en mode sécurisé point à point comme représenté à la figure 1.

A l'étape 206, l'organisme d'authentification 3 stocke les données transmises par le fournisseur de produits ou services 2 en attendant les informations complémentaires en provenance de l'intermédiaire neutre 4, avec pour clé, par exemple, l'identifiant de session et l'identifiant du fournisseur de produits ou services 2.

Simultanément aux étapes 205, 206, se déroule l'étape 207 selon laquelle l'utilisateur 1 est alors redirigé, selon des moyens bien connus de l'homme du métier, vers le site de l'intermédiaire neutre 2 en passant l'identifiant de session en paramètre.

Selon une variante, si le fournisseur de produits ou services 2 possède déjà le numéro de téléphone de l'utilisateur 1 ou bien s'il veut transmettre à l'intermédiaire 4 d'autres informations sur la transaction, comme par exemple la langue à utiliser ou le nombre de caractères à récupérer, il peut les lui transmettre en parallèle via une liaison sécurisée point à point 102.

A l'étape 208, si aucun numéro de téléphone ne lui a été transmis, l'intermédiaire neutre 4 demande à l'utilisateur 1 un numéro auquel ce dernier peut être contacté immédiatement. Il s'agit alors d'un numéro de téléphone fixe ou téléphone mobile.

Si nécessaire et pour des raisons de confort et d'interactivité, le numéro de téléphone peut être demandé à l'utilisateur 1, s'il n'a pas été transmis au préalable lors de l'étape 202 et transmis par l'utilisateur 1 à l'étape 203. Dans ce cas, lors de l'étape 207, le numéro est transmis à l'intermédiaire 4 de transaction.

A l'étape 209, l'intermédiaire neutre 4 gère tout ce qui concerne l'appel téléphonique et ceci comprend notamment la détection du mauvais format du numéro ou l'appartenance du numéro à une liste de numéros à risque. Il peut s'agir notamment des numéros de cabines téléphoniques sur la voie publique par exemple ou numéros utilisés lors de précédentes tentatives frauduleuses ou considérées comme risquées. L'intermédiaire neutre 4 gère également la détection d'occupation de ligne, la détection de numéros ou indicatifs internationaux inexistants, etc.

Des réponses appropriées à chaque cas sont apportées.

Par exemple, une correction du numéro de téléphone par l'utilisateur 1 est demandée. Il est possible aussi de fournir un rappel en différé et/ou en mode vocal, ou une annulation de la transaction.

L'intermédiaire neutre 4 vérifie aussi si l'utilisateur 1 utilise ce téléphone comme accès sur le réseau Internet 100. Dans ce cas, il est demandé à l'utilisateur 1 de terminer sa connexion Internet. Il est alors rappelé automatiquement, par exemple cinq minutes plus tard, et guidé dans les étapes 210 à 212 en mode vocal par exemple.

L'étape de fin de guidage vocal se termine alors par l'envoi d'un courrier électronique, avec une adresse - ou URL (Uniform Resource Locator) selon la terminologie anglo-saxonne – incluse, qui lui permet de poursuivre sa transaction une fois qu'il est reconnecté. Selon des variantes possibles, ce message électronique ou courriel (email selon la terminologie anglo-saxonne) peut être envoyé à l'issue des étapes 213 à 220 ou être remplacé par un lien au niveau de l'étape 209.

Selon une variante possible, si le numéro de carte de paiement de l'utilisateur 1 n'est pas validé par l'organisme d'authentification 3, alors l'intermédiaire neutre 4 rappelle l'utilisateur 1.

A l'étape 210, l'utilisateur 1 reçoit un appel téléphonique de la part de l'intermédiaire neutre 4. Il est guidé sur son terminal téléphonique et/ou sur son terminal web. Les messages pouvant être coordonnés et synchronisés entre les deux réseaux par les moyens de l'intermédiaire neutre 4.

A l'étape 211, l'utilisateur 1 entre sur son terminal 12, dans notre exemple le téléphone, les chiffres complémentaires des chiffres entrés sur

le réseau 100, dans notre exemple les huit derniers chiffres de son numéro de carte de paiement.

Il valide l'entrée des numéros sur son terminal 12, par exemple en appuyant sur la touche '#'.

Si le téléphone 12 de l'utilisateur 1 n'est pas à fréquence vocale, alors il peut selon une variante du procédé entrer les numéros via un système de reconnaissance vocale.

Lors de l'étape 212, l'intermédiaire neutre 4 vérifie qu'il a bien reçu le bon nombre de chiffres, à savoir dans notre exemple huit, puis la connexion téléphonique sur le réseau 200 est terminée. Il invite éventuellement l'utilisateur 1 à corriger les erreurs, par exemple de saisie de numéro.

L'empreinte numérique du couple numéro de téléphone + huit derniers chiffres du numéro de carte de paiement est stockée et utilisée pour identifier de manière anonyme l'utilisateur 1 lors des utilisations suivantes.

En variante, lors de la première transaction avec l'intermédiaire neutre 4, l'utilisateur 1 entre un code additionnel dit code personnel, soit en reprenant un code qui lui serait fournis par ailleurs, soit en composant un code de son choix lors de la première transaction.

L'empreinte numérique du couple numéro de téléphone + code personnel est stockée et utilisée pour identifier de manière anonyme l'utilisateur 1 lors des utilisations suivantes.

En variante également, le code personnel est remplacé par une signature vocale. L'utilisateur 1 en fin de transaction est amené à prononcer son nom. Cette signature vocale est stockée et pourra être utilisée en cas de litige.

Selon encore une variante, le code personnel est remplacé par une empreinte vocale au choix de l'utilisateur ou prédéfinie.

Lors des utilisations suivantes du couple numéro de téléphone + huit derniers chiffres du numéro de carte de paiement reconnu automatiquement par comparaison d'empreinte numérique, le code personnel sera redemandé et validé par comparaison avec l'empreinte numérique du couple numéro de téléphone + code personnel.

A l'étape 213, l'intermédiaire neutre 4 transmet à l'organisme d'authentification 3 les huit derniers chiffres reçus et l'identifiant de session en mode sécurisé point à point.

Lors de l'étape 214, l'organisme d'authentification 3 reçoit les données. Grâce à l'identifiant de session, l'organisme d'authentification 3 retrouve les huit premiers chiffres du numéro de carte de paiement précédemment stocké lors de l'étape 206.

Lors de l'étape 215, le numéro de carte de paiement complet est reconstitué par l'organisme d'authentification 3.

A l'étape 216, l'organisme d'authentification 3 valide ou ne valide pas la transaction et génère une réponse.

En 217, la réponse est transmise parallèlement par une transmission sécurisée point à point 106 vers le fournisseur de produits ou services 3 et éventuellement l'intermédiaire neutre 4 via une transmission sécurisée point à point 105.

Ensuite, lors de l'étape 218, l'intermédiaire neutre 4 envoie éventuellement le numéro de téléphone ayant servi à la transaction au fournisseur de produits ou services 2, via une transmission sécurisée point à point 102. C'est un numéro de téléphone valide et bien lié à l'utilisateur 1, qui constitue ainsi une trace de l'utilisateur 1. Ce numéro n'est pas stocké en clair chez l'intermédiaire neutre 4 sauf en cas de fraude. Il est stocké sous forme incomplète, par exemple avec deux chiffres masqués dans un fichier de trace de l'intermédiaire neutre 4 dans un but de facturation. Il est aussi stocké sous forme d'empreinte numérique dans des moyens formant base de données de l'intermédiaire neutre 4.

En 219, l'intermédiaire neutre 4 termine le dialogue avec l'utilisateur 1. L'utilisateur 1 est alors redirigé, selon des moyens bien connus de l'homme du métier, vers le site du fournisseur de produits ou services 2 en passant l'identifiant de session en paramètre.

Enfin en 220, le fournisseur de produits ou services 2 termine la transaction avec l'utilisateur 1, par exemple en confirmant la transaction.

Comme indiqué plus haut dans la description, selon une variante préférée, l'intermédiaire neutre 4 peut stocker une empreinte du numéro de

téléphone + les huit derniers chiffres du numéro de carte de paiement, lui permettant de construire un historique anonyme des transactions et d'y associer des données statistiques.

De plus l'intermédiaire neutre 4 peut également transmettre en temps réel au fournisseur de produits ou services 2 ainsi qu'à l'organisme d'authentification 3 un score ou des statistiques diverses concernant l'historique des transactions utilisant ce couple numéro de téléphone + huit derniers chiffres du numéro de carte de paiement. Les informations ainsi transmises peuvent permettre au fournisseur de produits ou services 2 de décider en temps réel de terminer ou de ne pas terminer la transaction. Les fraudes sont ainsi limitées pour le fournisseur de produits ou de services 2 mais aussi pour l'organisme authentification 3.

Ainsi, le procédé selon l'invention possède de nombreux avantages, dont notamment le fait d'utiliser des voies de transmission classiques et facilement accessibles telles que

- des transmissions sur le réseau Internet 100 ouvert, dont l'accès est relativement aisé. Ces transmissions peuvent être éventuellement sécurisées.
- des transmissions dites point à point entre deux sites certifiés qui peuvent transiter, soit via le réseau Internet avec des procédés de scellement de données, de cryptage et/ou d'échange de clés ou certificats, soit sur d'autres réseaux, notamment privés, garantissant une confidentialité point à point 300. Ces transmissions sont privatives entre des professionnels reconnus (les organismes d'authentification notamment les banques, leurs prestataires agréés).
- enfin des liaisons aboutissant sur le réseau téléphonique 200.

Seul le destinataire final, l'organisme d'authentification 3 a accès à l'ensemble des informations confidentielles.

L'intermédiaire 4 est neutre ne connaît rien d'autre de l'utilisateur que son numéro de téléphone et il n'a même pas besoin de stocker ce numéro de téléphone en clair ou crypté de manière réversible.

Avantageusement, l'intermédiaire neutre 4 peut appeler des utilisateurs 1 dans le monde entier. Dans ce cas, avantageusement, la grandeur du réseau 200 est transparente pour chaque utilisateur 1. Le réseau 200 s'adapte ainsi au réseau 100 qui est souvent à l'échelle mondiale, pour Internet notamment.

Toutes les étapes du procédé sont automatisées, sans intervention humaine et interactives.

Dans une mise en œuvre préférée, tout au long du déroulement du procédé, l'utilisateur 1 reste en contact simultané sur Internet via les moyens 41 de l'intermédiaire neutre 4, et la liaison téléphonique 200 avec les moyens 42 de l'intermédiaire neutre 4.

Les transactions sont hautement sécurisées par le système du rappel de l'utilisateur 1 par l'intermédiaire neutre 4.

L'utilisateur méfiant peut mémoriser le numéro de téléphone qui l'a rappelé s'il a un affichage des appels entrants, ou l'obtenir par prestation de service des opérateurs de téléphonie afin de vérifier l'identité du serveur appelant.

REVENDICATIONS

1. Procédé de transmission sécurisée et automatisée d'une information confidentielle, notamment d'un code d'identification, à un organisme d'authentification (3) lors d'une transaction avec un utilisateur (1) selon lequel on transmet une première partie d'une information confidentielle à l'organisme d'authentification sur un premier réseau, caractérisé en ce qu'il comporte une étape selon laquelle l'utilisateur (1) transmet la deuxième partie de l'information confidentielle, complémentaire de la première partie, à un intermédiaire neutre (4) sur un deuxième réseau (200) disjoint du premier réseau, l'intermédiaire neutre (4) transmettant ensuite à l'organisme d'authentification (3), sur un troisième réseau (300), la partie complémentaire de l'information confidentielle qu'il a reçue.

2. Procédé selon la revendication 1, caractérisé en ce que la saisie des deux parties complémentaires se fait sur des terminaux disjoints.

3. Procédé selon l'une des revendications 1 ou 2, caractérisé en ce que la transmission de la première partie de l'information confidentielle à l'organisme d'authentification (3) s'effectue directement entre l'utilisateur (1) et ledit organisme (3) sur le premier réseau.

4. Procédé selon l'une des revendication 1 ou 2, caractérisé en ce que la transmission de la première partie de l'information confidentielle à l'organisme d'authentification (3) s'effectue selon les étapes suivantes :

- l'utilisateur (1) transmet la première partie de l'information confidentielle à un fournisseur de produits ou de services (2) sur le premier réseau (100) ;
- le fournisseur (2) transmet ensuite la première partie à l'organisme (3) sur un troisième réseau (300).

5. Procédé selon l'une des revendications 1 à 4, caractérisé en ce qu'au moins un identifiant de session, partagés entre au moins deux des acteurs

(1, 2, 3, 4) de la transaction, permettent à l'organisme d'authentification (3) de reconstituer automatiquement l'information confidentielle que l'utilisateur (1) lui transmet.

6. Procédé selon la revendication 5, caractérisé en ce que chaque identifiant de session est généré par au moins un des acteurs (1, 2, 3, 4) de la transaction.

7. Procédé selon l'une des revendications 1 à 6, caractérisé en ce que des coordonnées de rappel de l'utilisateur (1) sur le deuxième réseau (200) sont transmises à l'intermédiaire neutre (4) par l'organisme d'authentification (3) sur le troisième réseau (300).

8. Procédé selon l'une des revendications 1 à 6, caractérisé en ce que des coordonnées de rappel de l'utilisateur (1) sur le deuxième réseau (200) sont transmises à l'intermédiaire neutre (4) par le fournisseur (2) de produits ou services sur le troisième réseau (300).

9. Procédé selon l'une des revendications 1 à 8, caractérisé en ce que la communication sur le premier réseau (100) entre l'utilisateur (1) et l'organisme d'authentification (3) ou le fournisseur de produits ou de service (2) est transférée automatiquement vers l'intermédiaire neutre (4) de transaction.

10. Procédé selon la revendication 9, caractérisé en ce que des coordonnées de rappel de l'utilisateur (1) sur le deuxième réseau (200) sont transmises à l'intermédiaire neutre (4) par l'utilisateur (1) sur le premier réseau (100).

11. Procédé selon l'une des revendications 1 à 10, caractérisé en ce que l'intermédiaire neutre (4) contacte automatiquement l'utilisateur (1) sur le deuxième réseau (200) pour récupérer la deuxième partie complémentaire de l'information confidentielle.

12. Procédé selon l'une des revendications 1 à 6, caractérisé en ce que l'utilisateur (1) contacte l'intermédiaire neutre (4) sur le réseau (200) pour transmettre la deuxième partie complémentaire de l'information confidentielle associée avec un identifiant de session.

13. Procédé selon l'une des revendications 1 à 12, caractérisé en ce que le troisième réseau (300) est un réseau sécurisé point à point.

14. Procédé selon l'une des revendications 1 à 13, caractérisé en ce que l'intermédiaire neutre (4) demande à l'utilisateur (1) de fournir, en outre de l'information confidentielle à transmettre à l'organisme (3), un code personnel qui permet d'identifier l'utilisateur (1).

15. Procédé selon la revendication 14, caractérisé en ce que le code personnel est transmis, par un réseau du type sécurisé point à point, à un deuxième organisme d'authentification auprès duquel l'utilisateur (1) est préalablement inscrit ou connu.

16 Procédé selon l'une des revendications 14 ou 15, caractérisé en ce que le code personnel est un code numérique et/ou vocal rentré sur un terminal (12) en connexion.

17. Procédé selon l'une des revendications 9 à 16, caractérisé en ce que l'utilisateur (1) est guidé automatiquement par l'intermédiaire neutre (4) dans les différentes étapes du procédé de transmission de la deuxième partie de l'information confidentielle sur le premier (100) et/ou deuxième (200) réseaux respectivement, de manière coordonnée et éventuellement synchronisée.

18. Procédé selon l'une des revendications 1 à 17, caractérisé en ce que l'utilisateur (1) est guidé automatiquement par les différents acteurs (2, 3, 4) de la transaction dans les différentes étapes d'échanges d'informations sur

les premier (100) et/ou deuxième (200) réseaux respectivement, de manière coordonnée et éventuellement synchronisée.

19. Procédé selon l'une des revendications 1 à 18, caractérisé en ce que l'intermédiaire neutre (4) et/ou l'organisme (3) stocke(nt) en clair ou en crypté de manière réversible les coordonnées de l'utilisateur (1).

20. Procédé selon l'une des revendications 1 à 19, caractérisé en ce que l'intermédiaire neutre (4) et/ou l'organisme (3) stocke(nt) en clair ou de manière réversible la deuxième partie complémentaire de l'information confidentielle fournie par l'utilisateur (1) sur le réseau (200).

21. Procédé selon l'une des revendication 14 à 20, caractérisé en ce que l'intermédiaire neutre (4) et/ou l'organisme (3) stocke(nt) en clair ou de manière réversible le code personnel transmis par l'utilisateur (1).

22. Procédé selon l'une des revendications 1 à 21, caractérisé en ce que l'intermédiaire neutre (4) et/ou l'organisme (3) établit un historique des transactions.

23. Procédé selon la revendication 22, caractérisé en ce que l'historique établi par l'intermédiaire neutre (4) et/ou l'organisme (3) est anonyme.

24. Procédé selon la revendication 23, caractérisé en ce que l'anonymat de l'historique est assuré par un codage non décryptable d'une combinaison des coordonnées de l'utilisateur (1) sur le deuxième réseau (200) et de la deuxième partie de l'information confidentielle transmise par l'utilisateur (1) à l'intermédiaire neutre (4) sur le deuxième réseau (200).

25. Procédé selon les revendications 14 à 24 caractérisé en ce que le code personnel est stocké, éventuellement en combinaison avec les coordonnées de l'utilisateur sur le réseau (200) par un codage non décryptable.

26. Procédé selon l'une des revendications 22 à 25, caractérisé en ce que l'intermédiaire neutre (4) émet un avis lié à l'historique de transaction de l'utilisateur (1) sur le réseau (300).

27. Procédé selon l'une des revendications 7 à 26, caractérisé en ce que l'intermédiaire neutre (4) recontacte l'utilisateur (1) après que ce dernier s'est déconnecté du premier réseau (100), ladite connexion au premier réseau (100) étant rétablie une fois que la deuxième partie de l'information confidentielle a été transmise à l'intermédiaire neutre (4).

28. Système de transmission sécurisée d'une information confidentielle, notamment un code d'identification, à un organisme d'authentification (3) lors d'une transaction, comportant des moyens chez un utilisateur (1) en transaction avec des moyens chez un organisme d'authentification (3) et/ou des moyens (21) chez un fournisseur (2) de produits ou services, et des moyens (41) chez un intermédiaire neutre (4), caractérisé en ce que les moyens chez l'utilisateur (1) comporte des moyens (11) aptes à transmettre une première partie d'une information confidentielle aux moyens (21) chez le fournisseur (2) de produits ou services ou chez l'organisme (3) sur un premier réseau (100), les moyens chez l'utilisateur (1) comportant en outre des moyens (12) aptes à transmettre la deuxième partie complémentaire de l'information confidentielle à des moyens (42) chez l'intermédiaire neutre (4) sur le deuxième réseau (200), les moyens chez l'intermédiaire neutre (4) et/ou les moyens chez le fournisseur (2) comportant en outre des moyens (23, 43) aptes à transmettre la partie du code qu'ils ont reçue vers des moyens (33) chez l'organisme d'authentification (3).

29. Système selon la revendication 28, caractérisé en ce que le premier (100) et le deuxième (200) réseaux sont disjoints.

30. Système selon la revendication 29, caractérisé en ce que le premier (100) et le deuxième (200) réseaux utilisent des technologies et protocoles de communication différents.

31. Système selon l'une des revendications 28 à 30, caractérisé en ce que les moyens de saisie (11) sur le premier réseau (100) sont indépendants des moyens de saisie (12) sur le deuxième réseau (200).

32. Système selon l'une des revendications 28 à 31, caractérisé en ce que l'organisme d'authentification (3), l'intermédiaire neutre (4) et/ou le fournisseur (2) de produits ou services comportent des moyens aptes à générer ou gérer au moins un identifiant de session leur permettant d'échanger et/ou retrouver des informations sur la transaction et permettant à l'organisme (3) d'autorisation de reconstituer l'information confidentielle émise par l'utilisateur (1) par les moyens de saisie (11, 12) sur les premier et deuxième réseaux (100, 200).

33. Système selon l'une des revendications 28 à 32, caractérisé en ce que l'intermédiaire neutre (4) comporte des moyens (42, 44) aptes à contacter automatiquement les moyens de saisie (12) de l'utilisateur (1) sur le deuxième réseau (200) afin que l'utilisateur transmette la deuxième partie du code confidentiel.

34. Système selon l'une des revendications 28 à 33, caractérisé en ce que l'intermédiaire neutre (4) comporte des moyens aptes à générer des empreintes numériques ou un cryptage unidirectionnel.

35. Système selon l'une des revendications 28 à 34, caractérisé en ce que le fournisseur de produits ou services comporte des moyens aptes à transférer la communication sur le premier réseau (100) entre les moyens de saisie (11) chez l'utilisateur connectés à des moyens formant serveur (21) chez le fournisseur vers des moyens formant serveur (41) chez l'intermédiaire neutre (4), mettant ainsi automatiquement l'utilisateur (1) en

communication avec l'intermédiaire neutre (4) et permettant ainsi aux deux acteurs d'interagir.

36. Système selon l'une des revendications 28 à 35, caractérisé en ce que le fournisseur (2) de produits et services, l'organisme d'authentification (3) et l'intermédiaire neutre (4) comportent des moyens (23, 33, 43) permettant la transmission de données sécurisées point à point sur un troisième réseau (300).

37. Système selon l'une des revendications 28 à 36, caractérisé en ce que l'intermédiaire neutre (4) possède des moyens (41, 42, 43, 44) lui permettant de coordonner et/ou synchroniser les messages sur les réseaux (100, 200 et 300).

38. Système selon l'une des revendications 28 à 37, caractérisé en ce que l'intermédiaire neutre (4) et/ou l'organisme (3) comporte(nt) des moyens (44) aptes à stocker les informations fournies par l'utilisateur (1) et des statistiques d'utilisation du système.

39. Système selon l'une des revendications 28 à 38, caractérisé en ce que l'intermédiaire neutre (4) comporte des moyens (42) aptes à effectuer de la reconnaissance vocale et/ou de la synthèse vocale.

40. Système selon l'une des revendications 28 à 39, caractérisé en ce que l'utilisateur (1) comporte des moyens (12) aptes à contacter automatiquement les moyens formant serveur (42, 44) de l'intermédiaire neutre (4) sur le deuxième réseau (200) afin de transmettre la deuxième partie du code confidentiel.

41. Système selon l'une des revendications 28 à 40, caractérisé en ce que l'intermédiaire neutre (4) comporte des moyens aptes à être contactés par l'utilisateur (1) sur le deuxième réseau (200) pour permettre la transmission de la deuxième partie de l'information confidentielle.

42. Système selon l'une des revendications 28 à 41, caractérisé en ce que l'intermédiaire neutre (4) et/ou l'organisme (3) comporte(nt) des moyens aptes à identifier l'utilisateur dans un historique grâce au code confidentiel transmis lors de la transaction.

43. Système selon l'une des revendications 28 à 42, caractérisé en ce que de part sa position privilégiée, l'organisme d'authentification (3) comporte également les moyens de l'intermédiaire neutre (4).

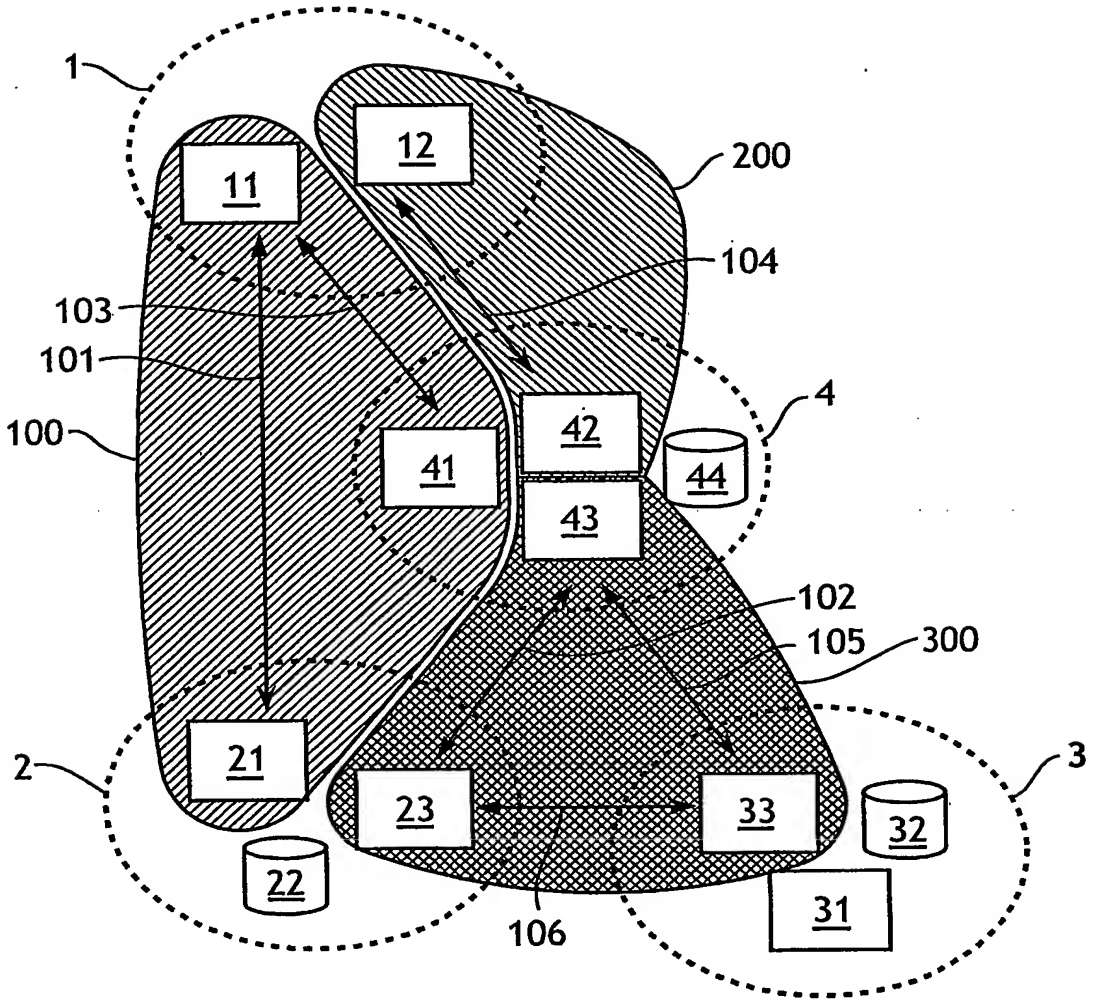

1
11
12
200
104
103
101
100
4
42
41
44
43
102
105
300
2
21
23
33
32
3
22
106
31

FIG.I

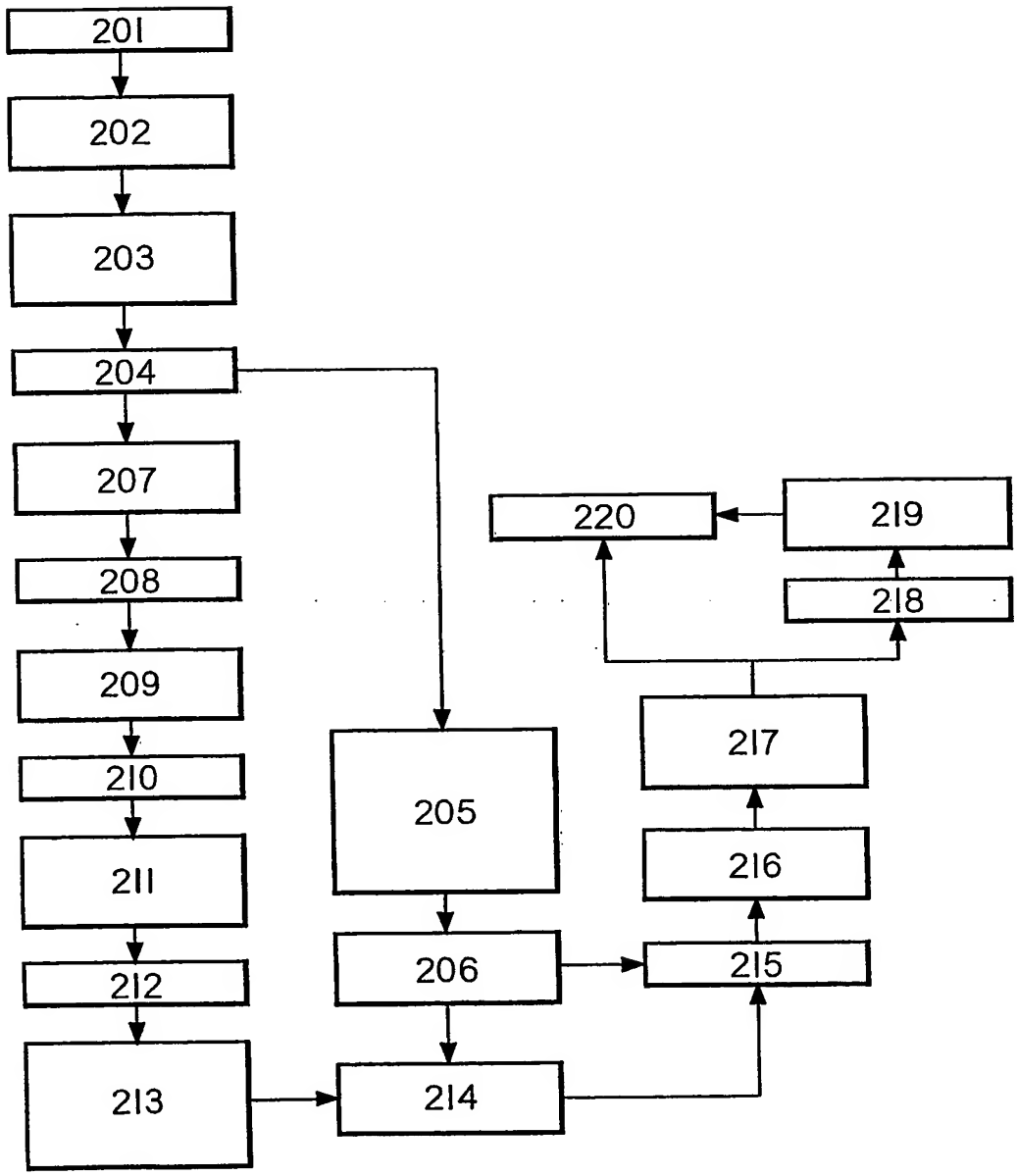

201
202
203
204
207
208
209
210
211
212
213
205
206
214
220
219
218
217
216
215

FIG.2

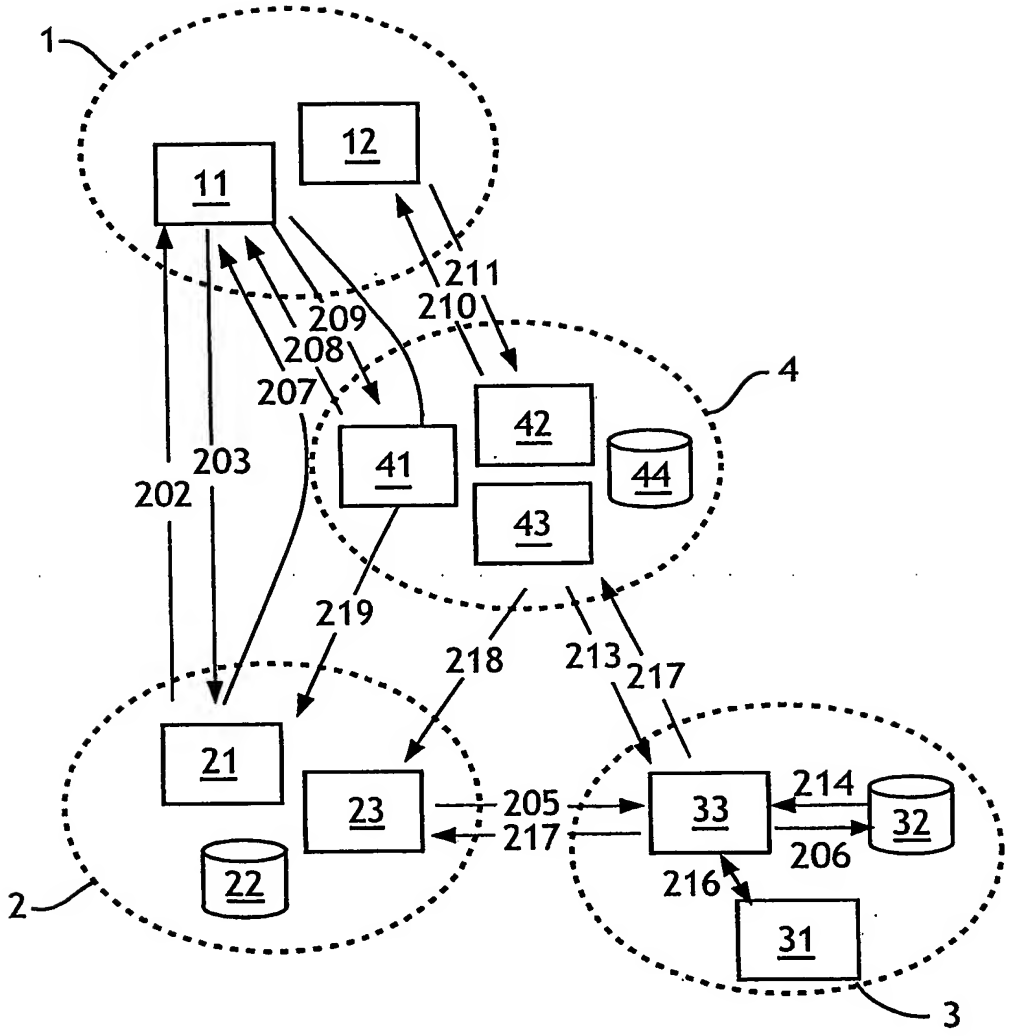

1
12
11
211
210
209
208
207
4
42
41
44
43
202
203
219
218
213
217
21
23
205
217
33
214
32
206
216
22
2
31
3

FIG.3

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 03/02536

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F19/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6 012 144 A (T.F. PICKETT) 4 January 2000 (2000-01-04) cited in the application the whole document	1-4, 7-13, 17-21, 28-31, 35-43
A	WO 96 29667 A (E. SANDBERG-DIMENT) 26 September 1996 (1996-09-26) cited in the application abstract; claims; figures	1-4, 7-13, 17-21, 28-31, 35-43

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 January 2004	29/01/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	David, J

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 03/02536

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	FR 2 806 229 A (M. SCHNEE) 14 September 2001 (2001-09-14) cited in the application abstract; claims; figure page 4, line 3 -page 7, line 20	1-4, 7-21, 28-31, 35-43
A	US 5 727 163 A (J.P. BEZOS) 10 March 1998 (1998-03-10) abstract; claims; figures	1,28
P,A	FR 2 828 966 A (SCHLUMBERGER SYSTEMS) 28 February 2003 (2003-02-28) the whole document	1,28
A	WO 01 28154 A (HELSINGIN PUHELIN) 19 April 2001 (2001-04-19)	
A	GB 2 332 833 A (INTERACTIVE MAGAZINES) 30 June 1999 (1999-06-30)	
A	US 6 070 154 A (O. TAVOR) 30 May 2000 (2000-05-30)	

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/FR 03/02536

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 6012144	A	04-01-2000	NONE		
WO 9629667	A	26-09-1996	US	5826245 A	20-10-1998
			AU	5366096 A	08-10-1996
			WO	9629667 A1	26-09-1996
FR 2806229	A	14-09-2001	FR	2806229 A1	14-09-2001
US 5727163	A	10-03-1998	US	5715399 A	03-02-1998
			US	6615226 B1	02-09-2003
FR 2828966	A	28-02-2003	FR	2828966 A1	28-02-2003
WO 0128154	A	19-04-2001	FI	992204 A	14-04-2001
			AU	7926900 A	23-04-2001
			EP	1221224 A1	10-07-2002
			WO	0128154 A1	19-04-2001
GB 2332833	A	30-06-1999	AU	1775099 A	19-07-1999
			WO	9934547 A1	08-07-1999
US 6070154	A	30-05-2000	NONE		

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PC FR 03/02536

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G07F19/00

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G07F H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	US 6 012 144 A (T.F. PICKETT) 4 janvier 2000 (2000-01-04) cité dans la demande le document en entier	1-4, 7-13, 17-21, 28-31, 35-43
A	WO 96 29667 A (E. SANDBERG-DIMENT) 26 septembre 1996 (1996-09-26) cité dans la demande abrégé; revendications; figures	1-4, 7-13, 17-21, 28-31, 35-43

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
"E" document antérieur, mais publié à la date de dépôt international ou après cette date
"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée
"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
22 janvier 2004	29/01/2004

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	David, J

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR 03/02536

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	FR 2 806 229 A (M. SCHNEE) 14 septembre 2001 (2001-09-14) cité dans la demande abrégé; revendications; figure page 4, ligne 3 -page 7, ligne 20	1-4, 7-21, 28-31, 35-43
A	US 5 727 163 A (J.P. BEZOS) 10 mars 1998 (1998-03-10) abrégé; revendications; figures	1,28
P,A	FR 2 828 966 A (SCHLUMBERGER SYSTEMS) 28 février 2003 (2003-02-28) le document en entier	1,28
A	WO 01 28154 A (HELSINGIN PUHELIN) 19 avril 2001 (2001-04-19)	
A	GB 2 332 833 A (INTERACTIVE MAGAZINES) 30 juin 1999 (1999-06-30)	
A	US 6 070 154 A (O. TAVOR) 30 mai 2000 (2000-05-30)	

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR 03/02536

Renseignements relatifs membres de familles de brevets

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
US 6012144	A	04-01-2000	AUCUN		
WO 9629667	A	26-09-1996	US	5826245 A	20-10-1998
			AU	5366096 A	08-10-1996
			WO	9629667 A1	26-09-1996
FR 2806229	A	14-09-2001	FR	2806229 A1	14-09-2001
US 5727163	A	10-03-1998	US	5715399 A	03-02-1998
			US	6615226 B1	02-09-2003
FR 2828966	A	28-02-2003	FR	2828966 A1	28-02-2003
WO 0128154	A	19-04-2001	FI	992204 A	14-04-2001
			AU	7926900 A	23-04-2001
			EP	1221224 A1	10-07-2002
			WO	0128154 A1	19-04-2001
GB 2332833	A	30-06-1999	AU	1775099 A	19-07-1999
			WO	9934547 A1	08-07-1999
US 6070154	A	30-05-2000	AUCUN		